UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA, Plaintiff, v. John Kelsey Gammell, Defendant.	)	Case No. 17-cr-00134 (WMW-DTS) **DEFENDANT'S MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS SEIZED EVIDENCE**

INTRODUCTION

This Memorandum is submitted on behalf of defendant John Kelsey Gammell in support of his motion to suppress certain seized evidence.

FACTUAL BACKGROUND

Washburn Computer Group

The government asserts that from July 30, 2015 to September 2016, the website of the Washburn Computer Group experienced website interruptions. Criminal Compl. at ¶ 7 [Docket 1]. The FBI could not immediately ascertain an attacker based on its own research. *Id.* at ¶ 8. Nevertheless, the agency began issuing generalized subpoenas and search warrants.

The vDOS Hacker

The government asserts that in July 2016, an internet security researcher who was both "well-known" to the agency and purportedly published in the field provided the FBI with database research relevant to this case. *Id.* at ¶ 28. The government leaves the researcher unnamed. *Id.* The FBI asserts that the researcher provided the database "to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks

on victim websites." *See id.* The database contains highly confidential information including "user registrations, user logins, payment and subscription information, contact with users, and attacks conducted," all of which is highly confidential and private information. *Id.* It would be difficult if not impossible to obtain Mr. Gammell's private information unless the researcher obtained unauthorized access to the database.

The government utilized the researcher's purloined information to draft a raft of subpoenas and search warrants. Eventually, the government used the vDOS database and the fruits of that database to chart a trail it claims led to Mr. Gammell. *Id.* at ¶ 29. The unnamed researcher thus accomplished his purported goal to "assist in a criminal investigation." *Id*. at 28.

The Arrest and Remaining Searches

Agents arrested Mr. Gammell at the Affordable Inns in Wheat Ridge, Colorado using information gleaned from the vDOS database. Agents searched Mr. Gammell's hotel room, his parents' home, purported car, and other locations also using information originating from the vDOS database. Agents seized physical evidence, including a GPS device, from all locations.

LEGAL ARGUMENT

I. EVIDENCE SEIZED AS A RESULT OF THE IMPROPERLY OBTAINED VDOS DATABASE IS FRUIT OF THE POISONOUS TREE AND SHOULD BE SUPPRESSED UNDER THE FOURTH AMENDMENT.

The purloined database records the internet security researcher provided to the FBI in July 2016 included user registrations, user logins, payment and subscription information, contact with users, and attacks conducted, including information related to Mr. Gammell. *Id*. The researcher took this information in apparent violation of state and federal statutes protecting the privacy of personal identity information. *See* 2 C.F.R. § 200.79; Minn. Stat. § 325E.61. The researcher, "well known" to the government and admittedly trying to curry its favor, acted as its agent to take what the government knew it could not take directly. This the Constitution

prohibits. *See Skinner v. Railway Labor Exec. Ass'n*, 489 U.S. 602, 614 (1989) (searches and seizures prohibited by even uncompelled private persons acting as government instruments); *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971) (invaliding search and seizure made outside judicial process).

The government then used this vDOS information to break open its case and issue a tidal wave of further subpoenas, warrants, and the arrest warrant for Mr. Gammell. Every one of those government warrants and subpoenas issued after July 2016 is tainted by the fruit of the poisonous tree and should be suppressed. *See Wong Sun v. United States*, 371 U.S. 471 (1963). Mr. Gammell asks this Court to suppress any information emanating from the following warrants and subpoenas.

Subpoena	Description
12/12/2016	AUSA's Subpoena to testify before a grand jury directed to PayPal Holdings, Inc.
01/30/2017	AUSA's Subpoena to testify before a grand jury directed to CenturyLink Custodian of Records/CenturyLink Law Enforcement Support Group
01/13/2017	AUSA's Subpoena to testify before a grand jury directed to Microsoft Corporation (Hotmail)
05/16/2017	AUSA's Subpoena to testify before a grand jury directed to Integra Telecom
05/15/2017	AUSA's Subpoena to testify before a grand jury directed to Comcast

Search Warrant	Issued Date	Return Date	Items to be Seized
Google	9/2016	11/2016	Records, communications associated with xxxxxxxx@gmail.com
Twitter	9/2016	10/2016	Information as described for Twitter account xxxxxxxx
AT&T Wireless	4/2017	4/2017	Information about the location of cellular telephone for xxx-xxx-xxxx
Residence & Garage New Mexico Address	5/2017	5/2017	Records (as described) related to the Subject Offense
Affordable Inns	5/2017	6/2017	Records (as described) related to the Subject Offense
Buick Century	5/2017		Records (as described) related to the Subject Offense

Search Warrant	Issued Date	Return Date	Items to be Seized
Tracer, Inc.	6/2017	6/2017	Locker and package
Discount Storage	6/2017	6/2017	Records (as described) related to the Subject Offense and unrelated items
Samsung Galaxy cellular phone	6/2017	7/2017	Records (as described) related to the Subject Offense

II. EVIDENCE SEIZED FROM THE BUICK CENTURY WHICH EXCEEDED THE SCOPE OF THE WARRANT IN VIOLATION OF THE FOURTH AMENDMENT'S PARTICULARITY REQUIREMENT SHOULD BE SUPPRESSED.

On the same day of Mr. Gammell's arrest, agents executed a search of a Buick Century vehicle. The warrant application sought "any and all records" related to the "Subject Offense**."** Ex. A at 00002114**.** This included "any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information … called for by this warrant." *Id.* at 00002115. The government offered little further description of additional electronic items they wished to seize.

Agents seized a GPS device in the glove box of the vehicle. *See* Ex. B at 00001477. Agents searched the GPS contents without first obtaining a particularized warrant. The GPS led to further investigative activities and seizure, all of which should be suppressed as fruit of the poisonous tree.

The Fourth Amendment guarantees the people to be free from unreasonable searches and seizures.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV, § 1.

A warrant which fails the particularity requirement is unconstitutional. *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (invalidating search warrant failing to describe persons or things to be seized). The particularity requirement "makes general searches … impossible" because it "prevents the seizure of one thing under a warrant describing another." *United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014) (vacating conviction for government's unreasonable seizure of computer). The warrant did not direct the agent, with required particularity, to seize the GPS, which was compartmentalized away from plain view. Nor did the warrant cover the information accessed from the GPS history. This search and seizure of the GPS was illegal.[1]

Mr. Gammell urges the Court to suppress the evidence which flowed from the GPS as the warrant failed to state with particularity the areas to be searched and the items to be seized. *See United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (invalidating warrant for failing particularity requirement and evidence not in plain view)**.** Conduct such as this "poses one of the most significant threats to privacy in the twenty-first century." *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1087 (July 2002).

CONCLUSION

Based upon the on the foregoing, Mr. Gammell respectfully requests that the Court suppress the evidence described here including the evidence secured flowing from the improperly obtained vDOS database as well as the GPS system.

[1] The good faith exception under *United States v. Leon*, 468 U.S. 897 (1984) does not apply because this search also flowed from the improper vDOS database and an agent could not reasonably rely on a such a generalized description of a storage medium.

Dated: August 17, 2017

By s/Rachel K. Paulose

Rachel K. Paulose
DLA Piper LLP (US)
Attorney ID No. 0280902
80 South Eighth Street, Suite 2800
Minneapolis, Minnesota 55402-2013
Telephone: 612.524.3008
Facsimile: 612.524.3001
rachel.paulose@dlapiper.com

ATTORNEY FOR DEFENDANT

145015227.2